Listing of Claims:

1. (Currently Amended) An asymmetrical cryptographic method for protecting a hard-wired electronic logic chip against fraud in transactions between the electronic chip and an application, including calculating an authentication value V from input parameters in the electronic chip, said method comprising the steps of:

producing [[a]] at least one pseudo-random number r at the application prior to a transaction;

calculating, at the application prior to the transaction, ~~a corresponding parameter~~ parameters x corresponding to the at least one pseudo-random number r ~~at the application prior to the transaction~~, [[said]] each corresponding parameter x being linked to the pseudo-random number r by a mathematical relationship;

storing the corresponding parameter x in a data memory of the electronic chip prior to the transaction;

producing, at the chip, the pseudo-random number r specific to the transaction via a serial pseudo-random generator included in the chip, said chip reading the stored corresponding parameter x calculated by the application prior to the transaction;

sending from the chip to the application the corresponding parameter x calculated by the application prior to the transaction, which is linked to the pseudo-random number r by the mathematical relationship and stored in the data memory of the chip;

calculating, at the chip, a parameter y constituting an entire or a portion of the authentication value V via a serial function whose input parameters are at least

the random number r specific to the transaction and a private key s belonging to an asymmetrical pair of keys;

sending the authentication value V from the chip to the application; and

verifying, at the application, said authentication value V via a verification function whose input parameters consist of public parameters including at least a public key p.

2. (Previously Presented) The method according to claim 1, wherein producing the random number r specific to the transaction comprises:

mixing some or all of the input parameters via a mixing function and supplying a series of bits as an output of the mixing function;

changing a state of a finite state automaton from an old state to a new state in accordance with a function depending at least on the old state and a value of the series of bits; and

determining a series of random bits to form an entire or a portion of the random number r via an output function having input arguments including at least the state of the automaton.

3. (Previously Presented) The method according to claim 2, wherein one input parameter is a secret key K shared by the chip and the application and is stored in a protected memory region of the chip.

4. (Previously Presented) The method according to claim 1, wherein the mathematical relationship comprises a function g^r in a set G of items g provided with an operation having at least an associative property.

5. (Previously Presented) The method according to claim 4, wherein the set G is a group Z_n^* of positive or null integers less than n and prime with n, wherein n is a positive integer.

6. (Previously Presented) The method according to claim 4, wherein the set G is any elliptical curve constructed on any finite body.

7. (Previously Presented) The method according to claim 1, wherein the serial function is an arithmetical function executing operations from a list comprising addition, subtraction, and left-shifts or right-shifts.

8. (Previously Presented) The method according to claim 7, wherein the arithmetical function executes only addition.

9. (Previously Presented) The method according to claim 7, wherein the arithmetical function executes only subtraction.

10. (Previously Presented) The method according to claim 7, wherein the arithmetical function input arguments further include input parameters and the arithmetical function entails executing one of the operations $y = r$ and $y = r + s$ as a function of a value assigned by the application to an input parameter t of the serial function.

11. (Previously Presented) The method according to claim 10, wherein the mathematical relationship comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the verification function compares a result obtained by applying the verification function to the authentication value V with either the value x or the product of the value x and the public key p of the chip corresponding to its secret key s, as a function of the parameter t, which comprises testing one of the equations $g^y = x$ and $g^y = xp$, as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the function $p = g^s$.

12. (Previously Presented) The method according to claim 7, wherein the arithmetical function has, for further input arguments, input parameters and comprises executing the operation $y = r$ or the operation $y = r - s$ as a function of a value assigned by the application to an input parameter t of the serial function.

13. (Previously Presented) The method according to claim 12, wherein the mathematical equation comprises a verification function g^r in a set G of items g provided with an operation having at least the property of being associative and wherein the verification function compares the result obtained by applying the mathematical relationship to the authentication value V with

the value x or with the product of the value x and the public key p of the chip corresponding to its secret key s, as a function of the value of the parameter t, which comprises testing the equation $g^y = x$ or the equation $g^y.p = x$, as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the equation $p = g^s$.

14. (Previously Presented) The method according to claim 7, wherein the arithmetical relationship has, for further input arguments, input parameters and comprises executing the operation $y = r + 2^i s$ as a function of a value assigned by the application to an input parameter t of the serial function, said parameter t comprising a string of m bits in which only one bit t_i is equal to 1, m being a natural integer.

15. (Previously Presented) The method according to claim 14, wherein the mathematical relationship comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the verification function tests the equation $g^y = xp^{2^i}$, as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the function $p = g^s$.

16. (Previously Presented) The method according to claim 7, wherein the arithmetical function has for, further input arguments, input parameters and comprises executing the operation $y = r + 2^t s$ as a function of the value assigned by the application to an input parameter t of the serial function.

17. (Previously Presented) The method according to claim 16, wherein the mathematical relationship comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the verification function tests the equation $g^y = xp^{2^t}$, as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the function $p = g^s$.

18. (Previously Presented) The method according to claim 7, wherein the arithmetical function has, for further input arguments, input parameters and executes the operation $y = r + ts$ as a function of the value assigned by the application to an input parameter t of the serial function, where t is an integer.

19. (Previously Presented) The method according to claim 18, wherein the mathematical relationship comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the verification function compares the result obtained by applying the verification function to the authentication value V with the value x or the product of the value x and the public key p of the chip corresponding to its secret key s, as a function of the value of the parameter t, which comprises testing the equation $g^y = xp^t$, as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the function $p = g^s$.

20. (Previously Presented) The method according to claim 1, wherein the parameter x sent from the chip to the application is a result obtained by applying a hashing function to at least one item linked to the random number r by a mathematical relationship and to an optional field D containing data linked to the application.

21. (Previously Presented) The method according to claim 20, wherein the arithmetical function has, for further input arguments, input parameters and executes the operation $y = r + 2^i s$ as a function of the value assigned by the application to an input parameter t of the serial function, said parameter t comprising a string of m bits in which only one bit t_i is equal to 1, where m is a natural integer.

22. (Previously Presented) The method according to claim 21, wherein the mathematical relationship comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the verification function tests the relationship $h(g^y/p^{2^i},D) = x$, as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the function $p = g^s$.

23. (Previously Presented) The method according to claim 21, wherein the mathematical relationship comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the verification function tests the relationship $h(g^y . p^{2^i},D) = x$, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the function $p = g^{-s}$.

24. (Previously Presented) The method according to claim 20, wherein the arithmetical function has, for further input arguments, input parameters and executes the operation $y = r - 2^i s$ as a function of the value assigned by the application to an input parameter t of the serial function, said parameter t comprising a string of m bits in which only one bit t_i is equal to 1, where m is a natural integer.

25. (Previously Presented) The method according to claim 24, wherein the mathematical relationship comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the verification function tests the relationship $h(g^y . p^{2^i}, D) = x$, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the function $p = g^{-s}$.

26. (Previously Presented) The method according to claim 20, wherein the mathematical function comprises a verification function g^r in a set G of items g provided with an operation having at least an associative property and wherein the parameter x sent from the chip to the application is a result obtained by applying a relationship of $x = h(g^r, D)$, where D designates an optional field containing data linked to the application and h is the hashing function.

27. (Previously Presented) The method according to claim 26, wherein the serial function has input arguments comprised of input parameters and executes either the operation $y = r$ or the operation $y = r + s$ as a function of the value assigned by the application to an input parameter t of the serial function and wherein the verification function compares the value x to the value $h(g^y, D)$ or the value $h(g^y.p, D)$ as a function of the value of the parameter t, where y is equal to

the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the equation $p = g^{-s}$.

28. (Previously Presented) The method according to claim 26, wherein the serial function has, for input arguments, input parameters and executes one of the operation y = r and the operation y = r + s as a function of the value assigned by the application to an input parameter t of the serial function and wherein the verification function compares the value x to the value $h(g^y,D)$ or the value $h(g^y.p,D)$ as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the equation $p = g^{-s}$.

29. (Previously Presented) The method according to claim 26, wherein the serial function has, for input arguments, input parameters and executes one of the operation y = r and the operation y = r - s as a function of the value assigned by the application to an input parameter t of the serial function and wherein the verification function compares the value x to the value $h(g^y,D)$ or the value $h(g^y.p,D)$ as a function of the value of the parameter t, where y is equal to the authentication value V and p is the public key of the chip corresponding to its secret key s, as defined by the equation $p = g^{s}$.

30. (Previously Presented) The method according to claim 7, wherein the set G is the group Z_n^* of positive or null integers less than n and prime with n.

31. (Previously Presented) The method according to claim 7, wherein the set G is any elliptical curve constructed on any finite body.

32. (Previously Presented) A device including an electronic chip and configured to implement an asymmetrical cryptographic method for protecting the electronic chip against fraud in transactions between the electronic chip and an application, said chip reading one or more stored values of a parameter x calculated prior to a transaction by the application, and said parameter x being linked by a mathematical relationship to a value of a random number r, the method comprising the electronic chip calculating an authentication value V from input parameters, and said device comprising:

a serial pseudo-random generator for producing a random number r specific to the transaction;

first memory means for storing the one or more values of the parameter x calculated prior to the transaction by the application which are linked by the mathematical relationship to the value of the random number r;

means for sending the parameter x linked to the random number r specific to the transaction from the chip to the application;

means for executing a serial function having as input parameters at least the random number r specific to the transaction and a private key s belonging to an asymmetrical pair of keys and providing as output a parameter y; and

output means configured to construct an authentication value V from at least the parameter y.

33. (Canceled)